Submission in Response to the Request for Information (RFI) – National Privacy Research Strategy (NPRS)

Title: Advancing Ambient Privacy and Informational Self-determination as Key Components of a National Privacy Research Strategy

Authors: H. Patricia McKenna, Lee W. McKnight, and Sarah A. Chauncey

In responding to the four questions raised by the Request for Information (RFI) – National Privacy Research Strategy (NPRS), this submission:

a) Points to a scenario in the education sector giving rise to a personal data issue in response to *Q1: privacy objectives*;
b) Advances a rethinking of the privacy concept for 21st century environments [1], specifically in response to *Q2: assessment capabilities*;
c) Additionally and by extension, informational self-determination is addressed in relation to people-technology-information interactions in response to *Q3: multi-disciplinary approach*; and
d) An architecture implementing a "responsible use framework"; privacy preserving information systems; and incorporating technological advances affecting privacy perceptions, in response to Q4: *privacy architecture*.

Q1. Privacy objectives: The use of data to inform educational policy, strategy, instruction and learning aligns to a critical mission of US schools – to ensure that all students achieve to their fullest potential and are college and career ready.

Scenario – Education

The State of New York was one of nine pilot states that had agreed to partner with an outside vendor, the Gates-funded corporation, inBloom, Inc. The State of New York would act as a conduit to pass confidential and personally identifiable (PII), student and teacher data, (names and social security numbers, behavior issues, etc.), to inBloom. inBloom would store the data in an encrypted cloud based storage platform and share student data for the purposes of tracking and research. inBloom would synthesize student data with a stated goal of assisting school districts in targeting the needs of individual children and to facilitate individualized learning.

Privacy Problem

Data security immediately became an issue and a heated controversy over New York State's decision to use inBloom ensued. In January of 2014 the NYS Education Department announced that it would delay the upload of Personally Identifiable Data to inBloom. By March the NYS Legislature adopted budget bill, A8556-D-2013 that authorized school districts to opt out of sharing PII with —shared learning infrastructure service providers (i.e. third party vendors) and data dashboard operators. On April 21, 2014, inBloom announced that it would cease operating. inBloom states that it believes a campaign of misinformation has led to its demise.

Proposed Remedy

The Gates-funded corporation inBloom controversy could have been averted had student data been passed using an ID number that could only be tied back to actual students by New York State and the school district responsible for the students. A data dashboard that supports analysis and synthesis of data can be developed without incorporating personally identifiable information.

Q2. Assessment capabilities: Assessing privacy in 21st century technology-rich information environments requires a re-thinking of the privacy concept.

Concepts

If, as is claimed in a legal context, the privacy concept is in 'disarray' and "nobody can articulate what it means" [2], the NPRS RFI provides an opportunity to rethink, evolve, and advance current and emerging understandings of privacy. Weitzner [3] cites earlier definitions of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

Zuckerberg is quoted as saying that "if he were to create Facebook today, user information would by default be public" [4]. Turkle takes issue with Zuckerberg's claim that "privacy is no longer a relevant social norm" and questions "what is intimacy without privacy and what is democracy without privacy" [5]. Xu [6] reframes privacy for online environments noting the "highly dynamic social interactions with rich data exchange" that occur.

Dourish and Bell [7] observe that privacy is not a stable and universally understood concept but rather, it is dependent upon other factors such as context, culture, situations, technologies, and manifestations. Dourish and Bell [7] encourage a rethinking of privacy, proposing to move "beyond privacy" to reach an understanding of privacy and security as social products. This understanding seeks "to support the human social and cultural practices through which the whole complex of phenomena – privacy, security, risk, danger, secrecy, trust, identity, morality, and power – are managed and sustained."

McCullough [8] defines ambient as "that which surrounds but does not distract" and "a continuum of awareness and an awareness of continuum." Bowden [9] points to the ambient privacy paradox and relationship between people and systems. McCullough notes that as "the dynamic of participatory networks shift to street level" this will lead to questions such as, "what particular concerns arise with the ambient?" and the issue of "governing the ambient."

Capabilities and Models

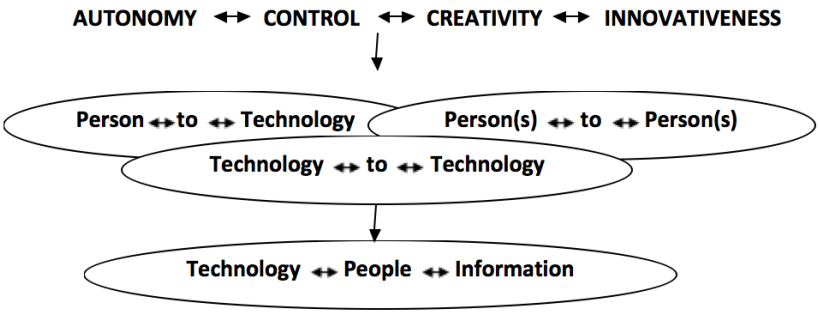
Based on Privacy by Design (PbD) principles, Cavoukian [10] argues that, "privacy cannot be assured solely by compliance with regulatory frameworks." Cavoukian

proposes continual adaptation and application of the PbD framework to organizational settings and everyday spaces. PbD accommodates legacy systems; encompasses the Big Privacy concept for big data environments; addresses personal data ecosystems (PDEs); and through partnering with business extends to BYOD (Bring Your Own Device) and other dynamic environments as a "privacy-aware mobility strategy."

Exploratory research conducted with early stage aware-enabled wireless grids provides an example of contemporary social media environments and emerging and next generation technologies [11]. Insights from this research contribute to development of the ambient privacy concept as a way of understanding and assessing emerging notions of people-technology-information interactions as continuous, adaptive, collaborative, and cross-boundary.

Fig. 1 illustrates the ambient privacy interaction dynamic, encompassing the constructs of autonomy, control, creativity, and innovativeness supporting the relationships (person to technology - person to person – technology to technology), which contribute to the technology-people-information dynamic.

Fig. 1 Ambient Privacy Interaction Dynamic

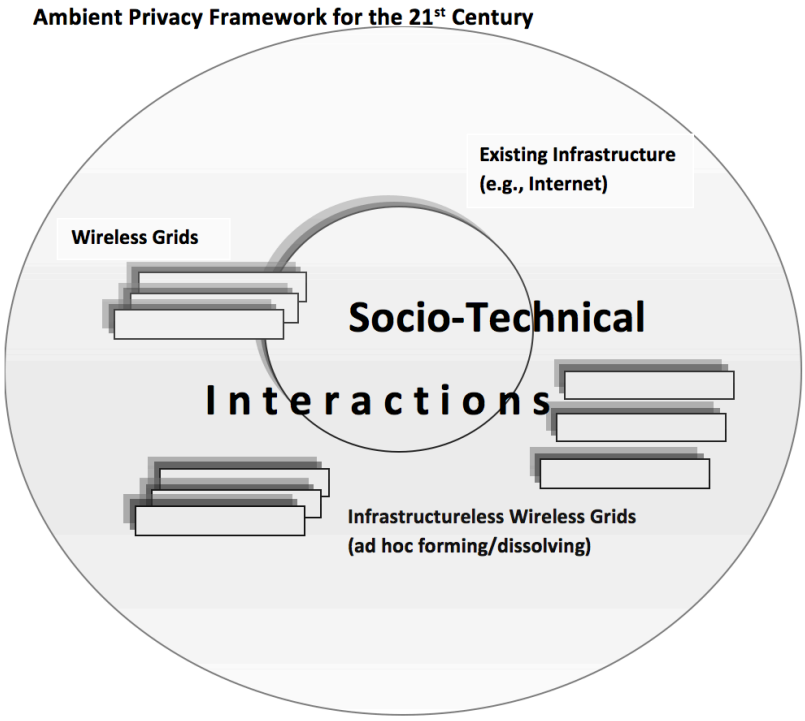


Ambient privacy complements and extends privacy in that it accommodates an interweaving of elements, characteristic of complex interactions in the moment, contributing to the potential for smarter privacy. These elements include: ad hoc, adaptive, analytics, collaborative, dynamic, fluid, learning, openness, participative, personalized, sharing, social, and trust.

Fig. 2 offers an ambient privacy framework for complex socio-technical interactions within existing infrastructures such as the Internet. The framework also adapts to any emerging and next generation technology such as wireless grids, designed to operate within existing infrastructures and as well, in ad hoc infrastructureless spaces.

As shown in the lower right of Fig 2., McKnight describes this scenario as "the dynamic inter-operation, integration, and dis-integration of networks, applications, and users, in real time" [12].

Fig. 2 Ambient Privacy Framework



Assessment Methods

The Consensual Assessment Technique (CAT) [13], used and studied widely in multiple domains for assessing creativity, may have relevance for assessments of ambient privacy. This is because the ambient privacy interaction dynamic (Fig. 1) contains the creativity construct and creativity is a critical component of innovative products and services. Recent early stage research explored the potential for application of the CAT in technology rich learning environments [14]. While the technique was found to hold promise in the learning and education domain, further, larger scale studies are required and encouraged across domains.

Risks, Benefits, and Mitigations

Rethinking risk, benefits, and mitigations in an ambient privacy context, it is worth noting that McCullough suggests, "it may be costly to neglect the role of augmented surroundings" [8]. In assessing and quantifying risks/benefits to privacy in an ambient privacy context, elements characteristic of complex interactions in technology-rich environments enumerated earlier in this paper must be taken into consideration. These elements include: ad hoc, adaptive, analytics, collaborative, dynamic, fluid, learning, openness, participative, personalized, sharing, social, and trust.

Similarly, evaluation of privacy risk mitigation in an ambient privacy context must consider the above-enumerated elements in determining the fulfillment of privacy requirements.

Q3. Multi-disciplinary approach: Informational self-determination emerges in the digital enlightenment discourse literature [15] in relation to data being generated in new and emerging information environments.

A key dimension of workplaces of the future [16] is the bringing together of many disciplines referred to as boundary-crossing and transdisciplinarity. Yoo [17] describes the connections between the fields of computing and law as "nacent and underdeveloped" and calls for an integration "of insights of both law and engineering in a pathbreaking and dynamic way" [17]. As if in response, Hildebrandt advances the ambient law concept [18], described as "an intelligent interplay between technological design and legal resolution." Explaining the privacy by design (PbD) concept in relation to informational self-determination, Cavoukian and Reed point to the importance of personal data and "control over how it is collected and used" [10]. Cavoukian and Reed note that, "privacy does not equal secrecy of personal data" but rather, that "it equates to individual control of one's data." In this sense, "privacy is not about keeping information secret (hiding information)", it is instead "about having a right to 'informational self-determination'."

An informational self-determination understanding of ambient privacy assists in understanding the ambient privacy interaction dynamic (Fig. 1) in terms of the constructs at play (autonomy-control-creativity-innovativeness); the reflexive and interactive relationships (people to technology, people to people, and technology to technology); and the resulting people-technology-information interaction dynamic.

Challenges and Objectives

Ambient privacy provides a context for framing challenges and objectives for cross-boundary thinking and transdisciplinarity [16] based on the elements characteristic of complex interactions in technology-rich environments enumerated earlier in this paper. These elements include: ad hoc, adaptive, analytics, collaborative, dynamic, fluid, learning, openness, participative, personalized, sharing, social, and trust.

As such, an ambient privacy perspective would strengthen contemporary and emerging understandings of privacy and have a stronger likelihood of:

a) Supporting innovation in cyberspace and in information systems and;
b) Supporting and accommodating diverse national/cultural perspectives on ambient privacy.

Q4. Privacy architecture: An architecture implementing a "responsible use framework" incorporating the three questions above (Q1 to Q3) is described below

based on the potential for adaptation and extension of the work of Massart and Shulman [19] with interaction data.

"Responsible use framework"

Building upon the education example provided in Q1, Massart and Shulman [19] describe a social data architecture based on a case study of the Learning Resource Exchange (LRE). As students and teachers use catalogs of Open Educational Resources (OERs), interaction data is collected and analyzed in real time to generate meaningful analytics. The architecture is designed to work across different systems and develops a method for unlocking, gathering, and aggregating interaction data.

To the extent that Massart and Shulman [19] use standards and protocols for metadata and paradata (interaction data which is a type of metadata), concern exists as articulated by this RFI for "encoding privacy policies in machine-checkable forms and ensuring their compliance and auditability; managing the collection, retention, and dissemination of sensitive data; and ensuring the confidentiality and integrity of sensitive data, while enabling desired uses."

Privacy-preserving information systems

However, Massart and Shulman [19] acknowledge that, "the issue of privacy is still largely unresolved and poses infinitely complex challenges for a global OERs exchange context, given the different laws in each jurisdiction."

Technological advances affecting privacy perceptions

Technological advances affecting privacy perceptions are offered in Q2 though a rethinking of the privacy concept for 21st century environments. The ambient privacy framework could be adapted to enhance and extend the work of Massart and Shulman [19] with interaction data. Introducing informational self-determination possibilities as described in Q3 contributes to emerging potentials for combining metadata and paradata for creative, innovative, and meaningful purposes within evolving notions of a 'responsible use framework'.

References

[1] McKenna, H. P., Arnone, M. P., Kaarst-Brown, M. L., McKnight, L. W., & Chauncey, S. A. (2013). Ambient privacy with wireless grids: Forging new concepts of relationship in 21st century information society. *International Journal for Information Security Research (IJISR)*, 3(1-2), pp. 408-417.

[2] Solove, D. J. (2006). A taxonomy of privacy. University of. *Pennsylvania Law Review*, 154(3), pp. 477-560.

[3] Weitzner, D. J. (2014). Accountable systems: Or, what does law have to do with computer science? Cambridge, MA: MIT. Retrieved 1 October 2014 from http://web.mit.edu/bigdata-priv/pdf/Daniel-Weitzner.pdf

[4] Kirkpatrick, M. (2010). Facebook's Zuckerberg says the age of privacy is over. *ReadWriteWeb,* January.

[5] Fleming, J., & Strainchamps, A. (2011). Transcript for Sherry Turkle on "Alone together." Wisconsin: ttbook.org. http://www.ttbook.org/book/transcript/transcript-sherry-turkle-alone-together

[6] Xu, H. (2012). Reframing privacy 2.0 in online social networks. *Journal of Constitutional Law*, 144, pp. 1077-1102.

[7] Dourish, P., Bell, G. (2011). *Divining a digital future: Mess and mythology in ubiquitous computing*. Cambridge, MA: MIT Press.

[8] McCullough, M. (2013). Ambient commons: Attention in the age of embodied information. Cambridge, MA: MIT Press.

[9] Cavoukian, A. (2014). Privacy by Design (PbD) framework. Toronto, ON: Privacy and Big Data Institute (PBD Institute), Ryerson University.

[10] Bowden, C. (2012). Privacy and autonomy in ambient intelligence. UK: LAAS ADREAM inauguration. Retrieved 1 October 2014 from http://www.laas.fr/files/ADREAM/3-Caspar_Bowden.pdf

[11] McKenna, H. P., Arnone, M. P., Kaarst-Brown, M. L., & McKnight, L. W. (2013). Ambient intelligence (AmI) with wireless grid enabled applications: A case study of the launch and first use experience of WeJay social radio in education. *Proceedings of the 7th International Technology, Education & Development (INTED) Conference*, pp. 1875-1884.

[12] McKnight, L. W. (2007). The future of the Internet is not the Internet: Open communications policy and the future wireless grid(s) (Workshop). Social and Economic Factors Shaping the Future of the Internet. Washington, DC: NSF/OECD.

[13] Hennessey, B. A., and Amabile, T. M. (2010). Creativity. Annual Review of Psychology, 61(1), pp. 569-598.

[14] McKenna, H. P., Arnone, M. P., Kaarst-Brown, M. L., McKnight, L. W., & Chauncey, S. A. (2013). Application of the consensual assessment technique in 21st century technology-pervasive learning environments. *Proceedings of the 6th International Conference of Education, Research and Innovation (iCERi2013)*, pp. 6410-6419.

[15] Hildebrandt , M., O'Hara, K., & Waidner, M. (2013). Introduction. In M. Hildebrandt, K. O'Hara, & M. Waidner (eds.), *Digital enlightenment yearbook 2013: The value of personal data*. Amsterdam, Netherlands: IOS Press.

[16] IFTF. (2011). Future work skills 2020. Palo Alto, CA: Institute for the Future for the University of Phoenix Research Institute.

[17] Yoo, C. S. (2014). Toward a closer integration of law and computer science. *Communications of the ACM*, 57(1), pp. 33-35.

[18] Hildebrandt, M. (2008). Defining profiling: A new type of knowledge. In M. Hildebrandt & S. Gutworth (eds.), Profiling the European citizen. London: Springer.

[19] Massart, D., and Shulman, E. (2013). Unlocking open educational resources (OERs) interaction data. *D-Lib Magazine*, 19(5/6).